Science & Society

EMBO reports

Export controls and the life sciences: controversy or opportunity?

Innovations in the life sciences' approach to export control suggest there are ways to disrupt biological weapons development by rogue states and terrorist groups without impeding research

Robert Shaw

In 2012, the scientific community became familiar with export controls and their application to biosecurity. In response to the controversy surrounding two publications of research that increased the human-to-human transmissibility of avian H5N1 flu virus, the Dutch government tried to use export control regulations to impede the publication of an article by microbiologist Ron Fouchier at Erasmus University in Rotterdam. This unique application of export controls sparked considerable debate among scientists as well as the community of specialists in export control and the nonproliferation of weapons of mass destruction (WMD). Regardless of where one stands on the question of whether the Dutch government's action was warranted, understanding the case's relationship with broader trends in export control and nonproliferation is important for practitioners in the life sciences. Export controls are not a passing trend, but have become a permanent feature in the regulatory landscape. However, the modern forms of controls to support security are still evolving and the life sciences themselves have introduced innovations that can further shape export controls to facilitate freedom of research while still promoting nonproliferation of WMD—nuclear, chemical, and biological.

While efforts to control trade for security or strategic purposes date back as far as Ancient Greece, modern export controls are rooted in the Cold War [1]. After World War II, NATO member states, Japan, and later Australia, organized the Coordinating Committee for Multilateral Export Controls (CoCom) to restrict exports of sensitive technology and materials from Western countries to the USSR and Eastern Bloc countries. CoCom member states compiled lists of dual-use goods and technologies that, while primarily commercial in nature, could significantly benefit military purposes. The more advanced the technology, the less likely the CoCom member states would permit its export to any of a group of "proscribed destinations"—namely the USSR and the Warsaw Pact states (Fig 1). At their heart, CoCom lists targeted manufactured hardware and electronics for control of their export to the Eastern Bloc: machine tools, materials, and later, lasers and semiconductors essential for the production of military hardware: tanks, fighter planes, and warships. Although it is difficult to measure its efficiency, elaborate efforts by the Soviet Union to acquire advanced multi-axis machine tools from suppliers in CoCom member countries suggested that the regime had some success in at least slowing transfers of sensitive items to the Eastern Bloc [2]. Biotech was only a small part of the control lists and only later during the export control regime's development. The US Master Export Security List from 1954, for instance, contained no reference to biological agents or related equipment.

> *"Export controls are not a passing trend, but have become a permanent feature in the regulatory landscape"*

CoCom ceased to function in 1994, but it served as a template for more inclusive export control "regimes" of countries cooperating to prevent the diversion of advanced dual-use technologies to WMD development programs, particularly in regions prone to conflict. These WMD-focused regimes began to form in the 1970s and 1980s in response to specific international events (Fig 2). India's 1974 nuclear test, described as a "peaceful" explosion and dubbed "Smiling Buddha", helped to create the "London Club" which later became known as the Nuclear Suppliers Group (NSG). A South Korean rocket launch in 1978 and similar tests by India in the 1980s resulted in the Missile Technology Control Regime (MTCR) in 1987. Most importantly for the life sciences, the Australia Group was created in response to the use of chemical weapons in the Iran–Iraq war and, in 1990, was augmented to control items relevant to biological WMD owing to concerns about the potential emergence of new state-level biological weapons (BW) programs, which were later confirmed by UN inspectors who discovered the extent of the Iraqi BW development effort during the 1980s. Today, the Australia Group coordinates the national export control policies of its member states to counter proliferation of both chemical and biological WMD. Its scope includes pathogens and biotech-related equipment, and it mirrors CoCom in terms of structure, operation, and use of control lists. As a consequence, the Australia Group's export controls trace their lineage to CoCom, which predominantly focused on hardware produced by large companies and shipped by well-established freight forwarders.

Middlebury Institute of International Studies at Monterey, Monterey, CA, USA. E-mail: rashaw@miis.edu
DOI 10.15252/embr.201642254 | Published online 16 March 2016

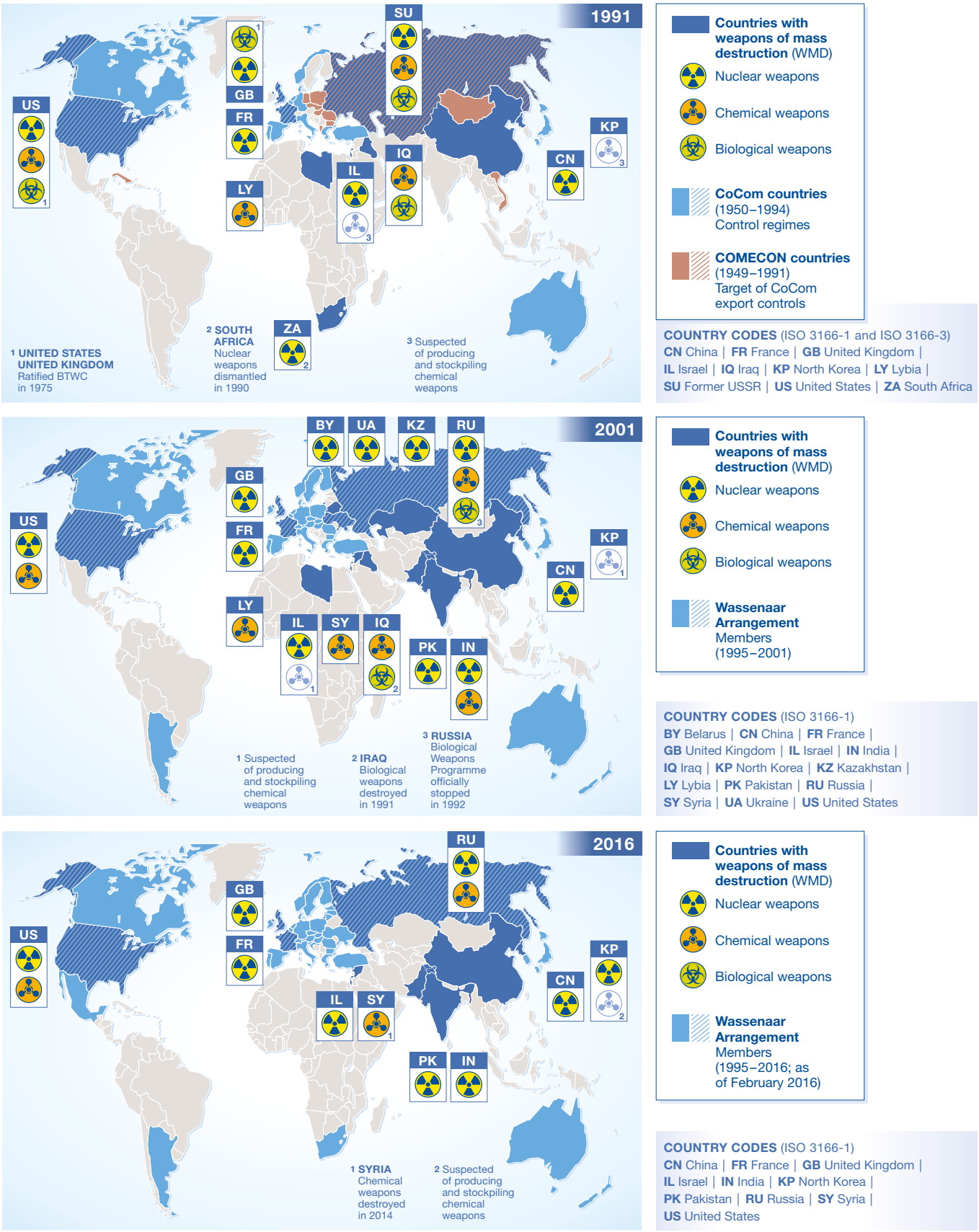
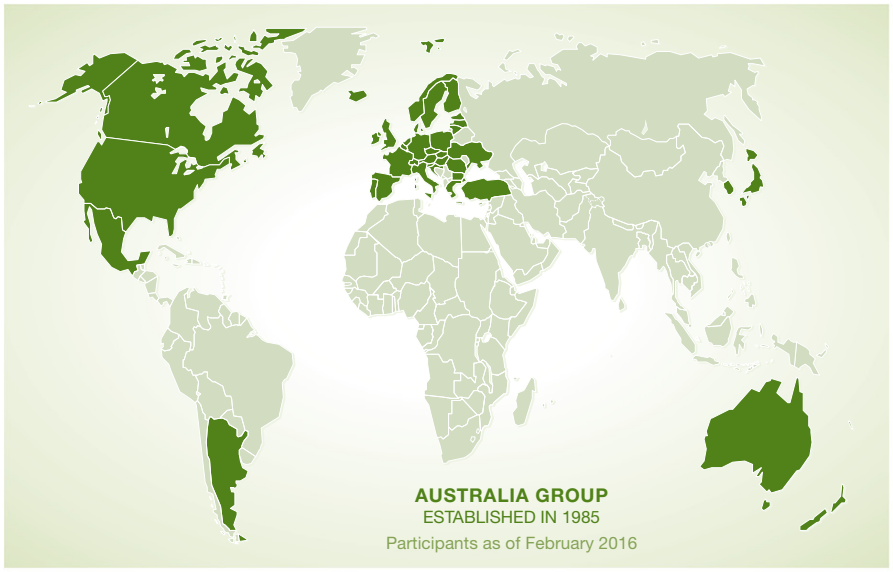


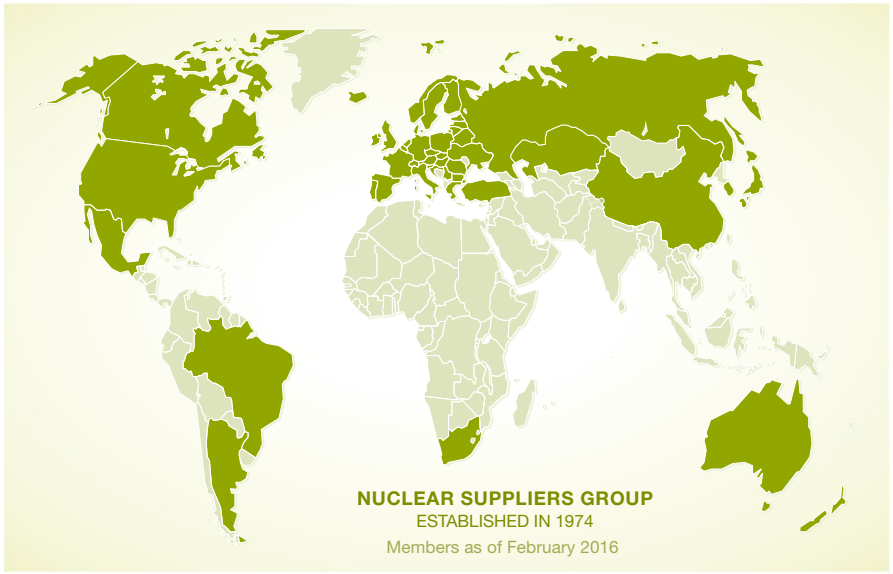
Figure 1. Countries in possession of Weapons of Mass Destruction and member states of control regimes during the Cold War, until 2001 and today.



AUSTRALIA GROUP

Argentina
Australia*
Austria
Belgium*
Bulgaria
Canada*
Croatia
Cyprus
Czech Republic
Denmark*
Estonia
European Union*
Finland
France*
Germany (West-G.*)
Greece*
Hungary
Iceland
Ireland*
Italy*
Japan*
Latvia
Lithuania
Luxembourg*
Malta
Mexico
Netherlands*
New Zealand*
Norway
Poland
Portugal*
Romania
Slovakia
Slovenia
South Korea
Spain*
Sweden
Switzerland
Turkey
Ukraine
United Kingdom*
United States*

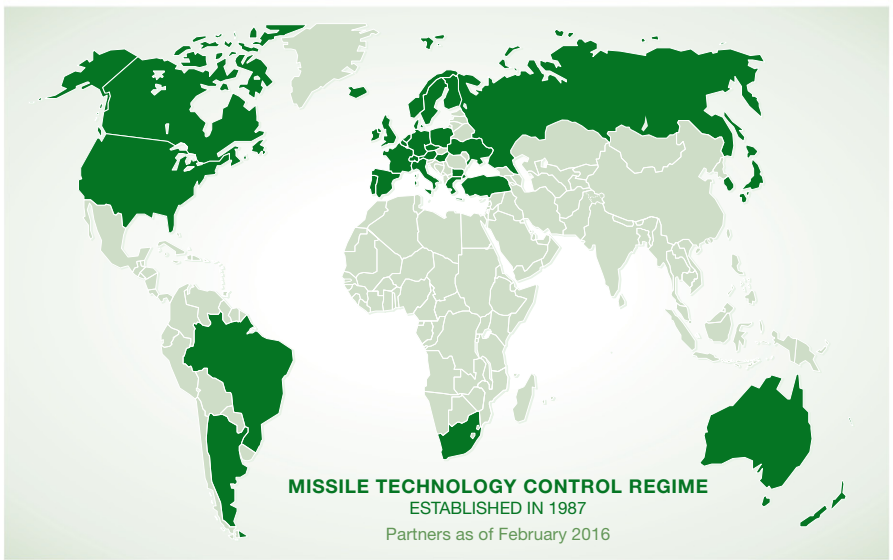
* Founding member



NUCLEAR SUPPLIERS GROUP

Argentina
Australia
Austria
Belarus
Belgium
Brazil
Bulgaria
Canada*
China
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France*
Germany (West-G.*)
Greece
Hungary
Iceland
Ireland
Italy
Japan*
Kazakhstan
South Korea
Latvia
Lithuania
Luxembourg
Malta
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Romania
Russia (USSR*)
Serbia
Slovakia
Slovenia
South Africa
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom*
United States*

* Founding member



MISSILE TECHNOLOGY CONTROL REGIME

Argentina
Australia
Austria
Belgium
Bulgaria
Brazil
Canada*
Czech Republic
Denmark
Finland
France*
Germany (West-G.*)
Greece
Hungary
Iceland
Ireland
Italy*
Japan*
Luxembourg
Netherlands
New Zealand
Norway
Poland
Portugal
South Korea
Russia
South Africa
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom*
United States*

* Founding member

Figure 2. Current member states of the Australia Group, Nuclear Suppliers Group, and the Missile Technology Control Regime.

As a tool to impede the proliferation of WMD, the control regimes have largely succeeded on a global scale. Nuclear Suppliers Group controls are a core component of UN Security Council nonproliferation sanction resolutions (such as those presently addressing North Korea's nuclear activities), and there is evidence that Australia Group controls impeded, to some degree, Libya's chemical weapons development programs in the 1990s and early 2000s [3]. However, since the early 2000s, these control regimes have faced new challenges in the forms of globalized supply chains, new means of sharing and disseminating intangible technology or "know-how"—for instance, via cloud computing—emerging manufacturing technologies such as 3D printing, and the explosion of online international trade platforms, most dramatically illustrated by e-commerce sites. Raymond Zilinskas and Phillipe Mauger describe in their recent article how the latter could enable would-be proliferators of WMD to avoid export controls of dual-use hardware to produce biological weapons [4]. Hardware production is moving from capital-intensive factories to small enterprises or even the home garage; international sales have moved from brick-and-mortar offices to the Internet, and shipping has shifted from venerable freight forwarders to a "one-click" selection from a menu of courier services. Additionally—and perhaps most importantly—these new modes of buying and shipping items are all available to terrorist organizations, some of which have expressed interest in acquiring WMD, most notably Al-Qaeda and ISIS.

> *"Unlike isotope centrifuges or missile parts, PCR machines and DNA synthesizers are cheap, widely used and easily available new or second hand"*

Export controls to inhibit research into or the production of biological WMD in particular face some unique challenges. Unlike isotope centrifuges or missile parts, PCR machines and DNA synthesizers are cheap, widely used and easily available new or second hand. Moreover, an increasing number of companies offer DNA and genome synthesis to academic, commercial, and even private customers. The same holds true for the equipment needed to produce and process biological agents: Fermenters, centrifuges, filtration units, or freeze-drying equipment are ubiquitous in food production and available from a wide range of suppliers, often outside export control mechanisms [4].

In response to these challenges—and at a significantly more global level than the limited membership of the export control regimes—the UN Security Council introduced Resolution 1540 in 2004, which requires all UN member states to introduce (or improve) and implement export controls with the specific aim of preventing terrorist organizations from acquiring WMD. The result has been, pardon the pun, a "proliferation" of export control laws and regulations. From the late 1990s to the 2000s, I was an export compliance specialist working for a large Japanese electronics firm, and we dealt mainly with USA and Japanese export regulations. Today, companies trading in Asia and the Near East have to deal with new or significantly upgraded export control laws and regulations in China, South Korea, Taiwan, Singapore, Malaysia, the Philippines, India, Pakistan, and the UAE in response to UNSCR1540—and the list of countries and legal frameworks in the region continues to grow. The EU has also significantly upgraded the export controls of member states through Regulation 428, "setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items", which incorporates all of the existing regimes' control lists—including those of the Australia Group. During the 2010s, the USA and Japan introduced new export control policies to specifically address cloud computing, and the USA and the EU have been discussing how to prevent transfers of intangible technology—the "know-how", typically in the form of knowledge that a scientist or engineer may possess, that is necessary to produce sensitive goods—to WMD proliferators more effectively.

This is the global security, political, and legal context against which the debate about the 2012 publications of H5N1 gain-of-function research emerged. The actions of the Dutch authorities and the ensuing, ongoing debate have occurred at a time when traditional notions of "manufacturer" and "exporter" are being eroded, just as new laws and regulations are blossoming and awareness of export controls is arguably at an unprecedented high. Quantifying "awareness" is of course difficult, but one measure is the issuance of UNSCR1540 implementation reports by UN member states. As of October 2004, only 59 states had submitted reports. Today, more than 100 states have submitted their reports. I have also observed increasing efforts by companies to introduce export compliance programs and hire staff. The industry-focused US Department of Commerce Annual Update Conference on Export Controls has had to move to a lottery-based system of registration, as the event has more registrants than its venues can accommodate.

> *"...applying "classic" export control measures to transfers of "intangible technology" [...] is notoriously difficult and can easily conflict with other laws or rights ..."*

With this in mind, the application of export controls to stall publication of Fouchier's article is perhaps not so surprising. Export controls are, after all, a nonproliferation tool and, from the Dutch authorities' perspective, it may have been the only one handy. However, applying "classic" export control measures to transfers of "intangible technology"—the knowledge of how to do something, rather than the equipment itself—is notoriously difficult and can easily conflict with other laws or rights, such as free speech or the publication of fundamental research. The latter has been an issue in the USA, where controls on "deemed exports"—transfers of technology from a US citizen or permanent resident to a foreign national—are regulated by a national export control system. Whether such "deemed exports" require an export license depends on the technology and the "destination"—that is, the home country of the foreign national—as well as whether the activity is considered "fundamental research" and thus exempt from restrictions. If the fundamental research exemption does not apply and if the technology is particularly sensitive, it can become legally necessary to restrict nationals of proscribed countries from participating in

certain US-based R&D activities. An investigation by the US Department of Commerce's Bureau of Industry and Security (BIS)'s Inspector General in 2004 to examine the efficacy and practicality of "deemed export" controls concluded that they needed to be strengthened. This generated strong reactions from technology companies and research institutions, and BIS established the Deemed Export Advisory Committee (DEAC) in 2006 to further investigate the issue. It reached a very different conclusion, arguing that US national security was harmed by inhibiting collaboration with global partners. Ultimately, in accordance with a recommendation of the DEAC, BIS announced the formation of an Emerging Technologies and Research Advisory Committee (ETRAC) in 2008—a body that meets regularly to consider deemed export issues.

> *"At the same time, the life sciences are well-positioned to stay ahead of these controversies and help shape the future of export controls"*

We can anticipate more such controversies in the future as export controls continue to develop globally in response to equally dynamic security challenges. Indeed, export control and nonproliferation practitioners and policy communities have examined the H5N1-related publications case in particular with much interest, recognizing that it has implications for future regulatory development and the need to balance security with the benefits of free trade and flow of information. One of the leading blogs in the USA for the trade compliance and legal practitioner community, Export Law Blog (http://www.exportlawblog.com/), has been following the case closely as it unfolded [5]. More recently, an article by Christos Charatsis examines the controversy in the inaugural issue of *Strategic Trade Review*—a peer-reviewed publication that, in itself, is an example of the growth of the export control field—and discusses the response by the EU and the USA and considers its impact for export control [6].

At the same time, the life sciences are well positioned to stay ahead of these controversies and help shape the future of export controls. The biotech sector can point to one of its security-related mechanisms—proactive screening of DNA synthesis orders for sequences from pathogens—as confirmation that this rapidly growing industry recognizes and squarely addresses the dual-use nature of its realm on a level that goes beyond what is seen in other industries. Shortly after leaving private industry in 2009, I initiated a project examining "red flag" guidance for export compliance programs and how it might be updated and augmented. National export control authorities typically publish lists of "red flag indicators" to help exporters identify suspicious purchase inquiries designed to circumvent export controls and divert dual-use goods to WMD or advanced military programs. The standard guidelines used by US export compliance practitioners is the "Know Your Customer" guidance in Part 732 of the Export Administration Regulations and similar guidelines exist in German, British, and other national authorities' export control regulations. This guidance consists of about a dozen examples of "red flags" that can indicate a suspicious inquiry: for example, a baking goods company asking for a quote for an advanced laser system (see Sidebar A). If a "red flag" is detected, the exporter is advised to seek more information about the customer, end-user, and end-use to confirm that it is a legitimate, legal transaction, or otherwise apply for an export license. While effective and applicable to nearly all industries, this "red flag" guidance is very general and has been largely unchanged since the mid-1990s.

> *"...the sophisticated dsDNA order screening practices are truly singular and demonstrate how proactive industry action shaped US regulatory development ..."*

Looking for any industry-specific indicators or "red flags", I came across the US Department of Health and Human Services' 2010 *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA*. I was stunned at the level of detail and the clearly defined steps to help suppliers of dsDNA identify suspicious queries, as well as the extensive intra-industry dialogue and debate that, at least in part, informed the development of this document. The division of screening into "customer", "sequence", and "follow-up", and the specific recommendations to report suspicious queries to the FBI exceeded the level of detail typically found in red flag guidance or "how-to" guides on building trade compliance programs for an exporting company, such as the US Department of Commerce's 2011 *Compliance Guidelines: How to Develop an Effective Export Management and Compliance Program and Manual*. Across all the US government training events that I had attended as an export compliance manager for more than a decade, I had not encountered anything this industry-specific or detailed.

> *"And awareness may be the best—or even the only—prescription for ensuring that today's entrepreneurs, thinkers, users of "the cloud" do not support, however unwittingly, WMD proliferation"*

Of particular interest was the *Screening Framework Guidance*'s incorporation of the Australia Group-based sections of the main US dual-use export control list to define an "Agent of Concern". In effect, a traditional export control tool—a control list—was incorporated into an innovative tool that is much better suited for 21st century globalized research and supply chains. Later, I learned of the background of the DHHS guidance and the intra-industry mechanisms—and extensive debates—that informed and paralleled its introduction [7]. While I imagine that controversy still persists—as perhaps evidenced by concerns about the effectiveness of this guidance in light of the potential for "split orders" (multiple orders for especially minute pieces of DNA that, in themselves would likely be undetectable under the *Screening Framework Guidance*, but could later be brought together and assembled to produce a pathogen) [8]—the energetic debate and competing initiatives within industry to promote order screening are all the more impressive, in that these actions truly exemplified the idea of self-regulation to a degree rarely seen in other

industry sectors. While many large firms across industries often "over-comply" by taking a conservative interpretation of export controls and avoiding some destinations or transactions even if technically legal, the sophisticated dsDNA order screening practices are truly singular and demonstrate how proactive industry action shaped US regulatory development in a manner that paralleled what companies were already doing, thereby reducing the likelihood of rushing ill-suited export controls into regulations. Notably, the DHHS guidance document was also inspired by a 2006 National Science Advisory Board (NSABB) document titled *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents* [9]. The NSABB, perhaps not coincidentally, was the body that, through the Dual-Use Review Committee, approached the H5N1 publication question in a different manner from the Dutch action by not invoking export controls.

Importantly, the debate surrounding the development of the *Screening Framework Guidance* and the more recent controversy over H5N1 research both increased awareness of export controls and, by extension, the importance of preventing WMD proliferation and terrorism. In the case of the former, export controls were also used as a component of what ultimately was a set of voluntary guidelines—a convenient mechanism for classifying and identifying certain "agents of concern". This creative co-opting of export controls represents an opportunity for the whole life sciences community. Highlighting such examples—however controversial screening strategies or their debated use may be—can inspire fresh thinking among export control policymakers, who struggle to keep up with developments in manufacturing, supply chain management, distribution, and research. It is an example of something less aimed at impeding/punishing potential violators and more as a framework to reinforce proactive awareness-raising goals. And awareness may be the best—or even the only—prescription for ensuring that today's entrepreneurs, thinkers, and users of "the cloud" do not support, however unwittingly, WMD proliferation.

A cautionary tale is unfolding today related to newly introduced export controls on "cyber-intrusion tools" as an element of cybersecurity, as agreed to by the successor of CoCom, the Wassenaar Arrangement, and then proposed for implementation, at the national level, by the US government. These controls have generated unprecedented protest from industry, placing the US government in the awkward position of having to reconcile its commitment to cybersecurity—in the form of updating regulations to reflect Wassenaar-agreed policy—with a pledge to industry to stall implementation of the provisions [10]. This is not to imply that the US information technology industry is to blame, but to highlight that extensive dialogue and building relationships with policymakers and government officials can reduce the negative impact of such controversies. The biosciences might also take its cue from the US aerospace industry which, when pressing

Sidebar A: Red flags and DNA screening

Red flags have been used to alert companies if and when a customer might divert an order toward criminal or terrorist use or if a company could be merely a façade for a state program to develop and produce WMD. These are examples of "red flags" that could indicate an unlawful use of an order:

- The customer or purchasing agent is reluctant to offer information about the end-use of a product.
- The product's capabilities do not fit the buyer's line of business; for example, a small bakery places an order for several sophisticated lasers.
- The product ordered is incompatible with the technical level of the country to which the product is being shipped. For example, semiconductor manufacturing equipment would be of little use in a country without an electronics industry.
- The customer has little or no business background.
- The customer is willing to pay cash for a very expensive item when the terms of the sale call for financing.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.
- Routine installation, training, or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- When questioned, the buyer is evasive or unclear about whether the purchased product is for domestic use, export, or reexport.

Source: "Know Your Customer" guidance of the US Export Administration Regulations. https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

In addition to using "red flag" criteria, companies that provide dsDNA molecules for academic, business, and private customers should implement additional screening procedures to make sure that the order is not being abused for developing biological weapons.

Providers should establish a comprehensive and integrated screening framework that includes both customer screening and sequence screening, as well as follow-up screening when customer and/or sequence screening raises a concern.

- Customer Screening: The purpose of customer screening is to establish the legitimacy of customers ordering synthetic dsDNA sequences. Providers should develop customer screening mechanisms to verify the legitimacy of a customer if the customer is an organization or confirm customer identity if the customer is an individual, to identify potential "red flags", and to conform to US trade restrictions and export control regulations.
- Sequence Screening: The purpose of sequence screening is to identify when "sequences of concern" are ordered. Identification of a "sequence of concern" does not necessarily imply that the order itself is of concern. Rather, when a "sequence of concern" is ordered, further follow-up procedures should be used to determine whether filling the order would raise concern. Sequence screening is recommended for all dsDNA orders.
- Follow-up Screening: The purpose of follow-up screening is to verify the legitimacy of customers both at the level of the customer and the principal user, to confirm that customers and principal users placing an order are acting within their authority, and to verify the legitimacy of the end-use.

Many customers will likely volunteer information about their identity or the sequence they are ordering. Providers should corroborate this information as part of their screening framework.

Source: "Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA" of the US Department of Health and Human Services. http://www.phe.gov/Preparedness/legal/guidance/syndna/Pages/default.aspx

for US export control reform, presented its recommendations as supportive of security rather than rehashing the standard (and tired) argument that US competiveness was being harmed by outdated controls. This approach contributed to convincing the Obama Administration to prioritize export control reform in 2010 with the launch of the President's Export Control Reform Initiative.

Ultimately—and reinforced by media coverage—export controls are here to stay. However, in light of accelerating technological and commercial innovations, their future application appears to shift toward reinforcing nonproliferation awareness rather than "controlling" trade. Ongoing security-focused efforts in the biosciences may offer policymakers a successful roadmap for this shift and thus a broader and more pragmatic way of thinking about the uncomfortable possibility of a rogue state or rogue individual misusing science, and therefore increasing the chances of its early detection.

Acknowledgements

I would like to thank John Lomicky for his assistance and insights in support of this article.

Conflict of interest

The author declares that he has no conflict of interest.

References

1. Cupitt RT (2000) *Reluctant Champions: Truman, Eisenhower, Bush, and Clinton: U.S. Presidential Policy and Strategic Export Controls*. New York: Routledge
2. Wrubel WA (1989) The Toshiba-Kongsberg incident: shortcomings of Cocom and recommendations for increased effectiveness of export controls to the east bloc. *Am Univ Int Law Rev* 4: 241 – 273
3. Seevaratnam JI (2006) The Australia Group. *Nonprolif Rev* 13: 401 – 415
4. Zilinskas RA, Mauger P (2015) E-commerce and biological weapons spread. *EMBO Rep* 16: 1415 – 1420
5. Burns C (2012) Bird Flu research flies into export laws, crashes, the burns. Export Law Blog
6. Charatsis C (2015) Setting the publication of "dual-use research" under the export authorisation process: the H5N1 case. *Strat Trade Rev* 1: 56 – 72
7. Tucker JB (2010) Double-edged DNA: preventing the misuse of gene synthesis. *Issu Sci Technol* 26: 23 – 32
8. Organization for Economic Co-operation and Development (2014) *Emerging Policy Issues in Synthetic Biology*, p. 121. http://www.oecd-ilibrary.org/science-and-technology/emerging-policy-issues-in-synthetic-biology_9789264208421-en
9. National Institutes of Health, US Department of Health and Human Services (2006) *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents*. http://osp.od.nih.gov/sites/default/files/resources/Final_NSABB_Report_on_Synthetic_Genomics.pdf
10. Burns C (2016) BIS still mulling over cybersecurity export rules. Export Law Blog

